REGULATORY OBSERVATION Resolution Plan	
RO Unique No.:	RO-UKHPR1000-0016
RO Title:	Demonstration of compliance with relevant good practice for control and instrumentation
Technical Area(s)	Control & Instrumentation
Revision:	Rev. 0
Overall RO Closure Date (Planned):	2021-03-31
Linked RQ(s)	-
Linked RO(s)	-
Related Technical Area(s)	- Electrical Engineering - Fault Studies
Other Related Documentation	Refer to Appendix A
Scope of Work	

Background

The requirement for duty holders to demonstrate that risks have been reduced as low as reasonably practicable (ALARP) is fundamental to the UK health and safety legislation and applies to the design, construction and operation of nuclear power plants. It is therefore an essential objective of the generic design assessment (GDA) for the requesting party's (RP's) nuclear safety submissions to demonstrate that risks have been reduced to ALARP. A key element of ALARP is the demonstration of the application of established relevant good practice (RGP).

For the Instrumentation and Control (I&C[1]) design of the UK Version of the Hua-long Pressurised Reactor (UK HPR1000), the level of substantiation of how the normative and informative requirements set out in the RGP have been addressed, is currently considered inadequate by the Office for Nuclear Regulation (ONR). The following issues regarding demonstration of the application of RGP in the I&C design of the UK HPR1000 have been identified:

- Some guides, codes or standards (e.g. NS-G-2.6, IEC 62566, etc.) that would be considered as RGP in a particular application have not been identified in the safety case;

[1] I&C is used in China, while C&I is used in the UK. The two are equivalent.

- There is a lack of a complete RGP list and justification of compliance with each RGP;
- There are no clear links in the safety case to where I&C operating experience (OPEX) has been considered, where OPEX is divided into two categories:
  - Feedback from international nuclear industry shared information and from previous GDA projects;
  - Relevant information from the reference plant design (Fangchenggang Unit 3 (FCG3)) on which the claims in the generic UK HPR1000 safety case depend.

ONR therefore raised RO-UKHPR1000-0016 to highlight these issues mentioned above.

ONR' s regulatory expectation is that the safety case for the UK HPR1000 generic design should adequately identify and address C&I RGP in the UK context, providing a clear 'line of sight' from the safety case claims to the detailed arguments and evidence. It should clearly identify where gaps or shortfalls against RGP exist and articulate how these impact the generic design. Any gaps should be adequately progressed to provide a robust demonstration that the UK HPR1000 C&I design reduces relevant risks to ALARP. Where claims are made that rely on evidence from the reference plant design, this should be clearly articulated in the arguments with links to the specific evidence provided. The relevant evidence should be provided to ONR in a way that provides a clear link to the claims and arguments and demonstrates how these are met.

To achieve this, as part of the resolution of this RO, the RP will need to undertake and document the following activities:

i. Identify the sources of C&I RGP in the UK context, and justify its applicability to the UK HPR1000 C&I design;

ii. Undertake a comprehensive comparison of the UK HPR1000 C&I design against the identified RGP and provide detailed justifications in the safety case of how the RGP is adequately addressed;

iii. Identify gaps against RGP for the UK HPR1000 generic design. The significance of any identified gaps should be articulated and an explanation of how these will be addressed during GDA should be provided. Plans and timescales for the application of the RP's ALARP methodologies should also be included in order to demonstrate the UK HPR1000 C&I design reduces risks to ALARP;

iv. Identify and provide any relevant information from the reference plant design (in the context of C&I) on which the claims in the generic UK HPR1000 safety case depend, including the following:

- *Its purpose and position in the safety case, including key links to other safety case*

documentation;

- *Detailed justification (i.e. arguments) the relevance of this information (i.e. evidence) and how it demonstrates that the safety case claims are addressed.*

Based on the relevant ONR *Safety Assessment Principles (SAPs)* [1] (e.g. ECS.3, ECS.5, etc.) and the ONR *Technical Assessment Guide (TAG)* on the demonstration of ALARP [2], the detailed identification and compliance justification against RGP for the generic UK HPR1000 I&C design will be developed. This includes the relevant information from the reference plant design related to the UK HPR1000 safety case. The application of the ALARP methodology in the UK HPR1000 I&C design will also be presented.

This resolution plan provides the intended tasks, deliverables and schedule that will be undertaken to address the concerns raised by ONR regarding the demonstration of compliance with RGP.

Scope of work

The scope of work is described as follows:

- Review of the codes and standards applicable to the UK HPR1000 I&C design with a justification of their applicability (including application scope, assessment and impact analysis);
- Review of OPEX from international nuclear industry shared information, previous GDA projects and FCG3 reference I&C design applicable to the UK HPR1000 with a justification of their applicability (including justification of how OPEX has been selected);
- Presentation of the reference design related to the UK HPR1000 safety case in Claims, Arguments and Evidence (CAE) structure;
- Presentation of the ALARP methodology applied in the UK HPR1000 I&C design.

For the closure of this Regulatory Observation (RO), the following documents will be updated or developed respectively:

a) The report '*ALARP Demonstration Report of PCSR Chapter 8*', summarises the identified RGP applicable to the UK HPR1000 I&C design as well as any potential improvements that result from the systematic review against RGP. This report will be updated and delivered in response to RO Action 1 and as part of the response to RO Action 3;

b) The document '*BSC of Protection System*', provides arguments and evidence related to the Reactor Protection System (RPS [PS]) to support the Pre-Construction Safety Report (PCSR). This report will be updated in response to RO Action 2;

c) The documents '*SAS System Requirement Specification*' and '*PSAS System Requirement Specification*', which specify the system requirements of the Safety Automation System (SAS)

and Plant Standard Automation System (PSAS), will be developed in response to RO Action 3.

The ALARP demonstration report is used as a working document to catalogue tasks from the iterative systematic review against RGP, and as such is a continuously evolving report.

Please note that, subject to regulatory agreement, this resolution plan may be updated in future.

Deliverable Description

RO-UKHPR1000-0016.A1 –Identification of relevant good practice

The RO action states that:

In response to this Regulatory Observation Action, General Nuclear System Limited should:

- *Identify all sources of RGP considered applicable to the UK HPR1000 C&I design and justify its applicability.*

Resolution Plan

ONR's regulatory expectation is that the safety case for the UK HPR1000 generic design should adequately identify all RGP applicable to the I&C design in the UK context. According to the *ALARP Methodology* [3], the RGP applicable to each topic area shall be sufficiently identified and used as a basis for undertaking a review of the holistic design to identify potential improvements on ALARP grounds.

Compared with the regulatory expectation and ALARP principle, the RGP applicable to the I&C design presented in the current UK HPR1000 safety case submission is not complete, specifically regarding OPEX from international nuclear industry shared information, previous GDA projects and relevant information from the reference plant design.

According to the principles from *Guidance on the Demonstration of ALARP (As Low As Reasonably Practicable)* [2] and *ALARP Methodology* [3], the following improvement work is intended to be undertaken:

a) Review of the identification and screening process of codes and standards, according to the principles in *General Principles for Application of Laws, Regulations, Codes and Standards* [4]. This review shall clearly identify any additional codes or standards that are applicable to the UK HPR1000 I&C design. The applicability of codes and standards will then be reviewed in a high-level manner considering several factors, e.g. the scope of application, degree of familiarity, application in practical engineering, relationship with the reference plant, etc.;

b) Review of OPEX from international nuclear industry shared information (e.g. Multinational Design Evaluation Programme (MDEP), Information System on Occupational Exposure (ISOE), etc.) and relevant ROs/Regulatory Issues (RIs)/Assessment Reports from previous GDA projects. The OPEX review will discuss the wider learning that has been incorporated (or will be considered/incorporated subject to ALARP assessments) into the UK HPR1000 design;

c) Identify and review relevant information from the documentation list and data from FCG3 reference I&C design to assess its applicability and usage within the UK HPR1000 safety case, i.e. as the evidence to support relevant claims and arguments.

In response to RO Action 1, the '*ALARP Demonstration Report of PCSR Chapter 8*' will be updated and summarise the RGP applicable to the UK HPR1000 I&C design. This report will include:

- A list of codes and standards applicable to the UK HPR1000 I&C design with a justification of their applicability;
- A list of OPEX from international nuclear industry shared information and previous GDA projects that has been incorporated (or will be considered/incorporated subject to ALARP assessments) into the UK HPR1000 I&C design with a justification of applicability;
- A list of OPEX from FCG3 reference I&C design that directly supports the UK HPR1000 safety case with a justification of applicability.

RO-UKHPR1000-0016.A2 –Identification of relevant reference design information

The RO action states that:

In response to this Regulatory Observation Action, General Nuclear System Limited should:

- *Identify all relevant evidence, including any information from the FCG3 C&I design, on which the claims made in the UK HPR1000 safety case depend, inluding its role in the safety case, the claims it supports and key links to other safety case documentation.*
- *Provide a clear trail from the safety case claims, through detailed arguments to the evidence that demonstrates that the claims are addressed.*

Resolution Plan

ONR's regulatory expectation is that claims relying on evidence from the reference plant design should be clearly articulated in the arguments, with links to the specific evidence provided. The relevant reference to the I&C design should be provided in a way that provides a clear link to the claims and arguments and demonstrates how these are met.

It is recognised that the reference I&C design information from FCG3, on which the claims of the UK HPR1000 depend, has not been presented clearly in the safety case to date. The improvement work is intended to provide a clear trail from the safety case claims relying on evidence from the

FCG3 reference I&C design, to the detailed arguments with links to the specific evidence.

As stated in RO Action 1, a list of OPEX from the FCG3 reference I&C design related to the UK HPR1000 safety case will be documented in the ALARP demonstration report. The information in this list will be integrated into each relevant Basis of Safety Case (BSC) document associated with the claims and arguments it supports.

To address RO Action 2, the RPS [PS] system will be used as an example case to incorporate the reference design information relevant to the UK HPR1000 safety case in CAE structure into the BSC document of the system. The RPS [PS] is proposed because the safety claims for the system rely heavily on reference design information. In particular, the functional requirements and control logic are mostly the same between the UK HPR1000 and FCG3. The complexity of the RPS [PS], along with the fact that other I&C systems for the UK HPR1000 have more significant differences to the reference design, makes the RPS [PS] the most appropriate and practical system to use for the demonstration. The FCG3 reference I&C design will continue to be analysed and integrated into other relevant updated BSC documents for GDA submissions as required to meet the GDA schedule.

In response to RO Action 2, the updated document '*BSC of Protection System*' will be provided.

RO-UKHPR1000-0016.A3 –Demonstration of compliance with relevant good practice

The RO action states that:

In response to this Regulatory Observation Action, General Nuclear System Limited should:

- *Undertake a complete and consistent comparison of the UK HPR1000 C&I design against the identified RGP, including both the normative and informative requirements of RGP.*
- *Provide detailed justification of compliance with the RGP.*
- *Identify any gaps or non-compliances against RGP, articulate their significance and provide an explanation of how they will be addressed in GDA.*
- *Provide a robust demonstration of how the UK HPR1000 C&I design reduces risks ALARP. Where the RP intends to justify a gap or non-compliance with RGP on ALARP grounds, this should demonstrate the options that were considered, why the selected option(s) achieve the optimum safety benefit, why other options were deselected and why measures to further reduce risks are not reasonably practicable.*

Resolution Plan

ONR's regulatory expectation is that the safety case should clearly identify where gaps or shortfalls against RGP exist and articulate how these impact the UK HPR1000 I&C generic design. According to the ONR TAG *Guidance on the Demonstration of ALARP (As Low As Reasonably Practicable)*

[2], any non-conformance with RGP should be explicitly highlighted and then justified as reducing risks to ALARP within the safety case.

The ALARP approach of the UK HPR1000 I&C design, in accordance with *Guidance on the Demonstration of ALARP (As Low As Reasonably Practicable)* [2], is to systematically review the UK HPR1000 I&C design against RGP, to collate the gaps and to undertake detailed specific ALARP assessment. The identified gaps will go through a detailed specific ALARP assessment to determine whether design modifications or other improvements are necessary to reduce risks to ALARP. The optioneering process will be described in individual optioneering reports. The report '*ALARP Demonstration Report of Chapter 8*' is a key document for implementing the ALARP approach. In response to RO Action 3, all identified gaps will be recorded and relevant optioneering submissions will be summarised in an updated '*ALARP Demonstration Report of Chapter 8*', with appropriate references provided.

In terms of specific implementation, the lack of requirement specification documents of the SAS and PSAS has been identified as a gap compared to IEC 61513 [5], resulting in a challenge to the management of functional requirements from different sources for the SAS and PSAS. This will be used as the example to demonstrate how gaps or non-compliance against RGP will be addressed in GDA and to close RO Action 3. The ALARP demonstration of any gap in other I&C systems will continue to be performed in the safety case as required to meet the GDA schedule.

In response to RO Action 3, the document '*ALARP Demonstration Report of Chapter 8*' will be updated. Additionally, the documents '*SAS System Requirement Specification*' and '*PSAS System Requirement Specification*' will be developed to ensure effective management of system requirements of the SAS and PSAS. The requirement specification of the SAS and PSAS will include:

- The functions of the system;
- The global performance requirements;
- The constraints on the design of the system;
- The boundaries and interfaces with other systems;
- The interfaces with the users;
- The environmental conditions applicable to the system;
- The qualification required.

Impact on the GDA Submissions

This GDA submissions that are impacted by this resolution plan include:

- *ALARP Demonstration Report of PCSR Chapter 8*,

- *BSC of Protection System*,
- *SAS System Requirement Specification*,
- *PSAS System Requirement Specification.*

Timetable and Milestone Programme Leading to the Deliverables

See attached Gantt Chart in APPENDIX A.

Reference

[1] ONR, Safety Assessment Principles for Nuclear Facilities, Revision 0, November 2014.

[2] ONR, Guidance on the Demonstration of ALARP (As Low As Reasonably Practicable), NS-TAST-GD-005, Revision 8, July 2017.

[3] CGN, ALARP Methodology, GHX00100051DOZJ03GN, Revision B, April 2018.

[4] CGN, General Principles for Application of Laws, Regulations, Codes and Standards, GHX00100018DOZJ03GN, Revision F, August 2018.

[5] IEC, Nuclear power plants - Instrumentation and control important to safety - General requirement for systems, IEC 61513, Revision 2, 2011.

PREVIOUS REVISIONS RECORD				
Rev.	**Author**	**Scope/Reason of Revision**	**Date**	**Page**

CGN EDF General Nuclear System	REGULATORY OBSERVATION RESOLUTION PLAN RO-UKHPR1000-0016	Rev.: 0	Page: **10 / 10**
		GDA-REC-GNS-005201	

APPENDIX A RO-UKHPR1000-0016 Gantt Chart

Tasks	Steps	2019					2020												2021		
		Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar
RO Action 1																					
Deliverable: ALARP Demonstration Report of PCSR Chapter 8, Rev. D	Development																				
	Submission										▲										
RO Action 2																					
Deliverable: BSC of Protection System, Rev. C	Development																				
	Submission											▲									
RO Action 3																					
Deliverable: ALARP Demonstration Report of PCSR Chapter 8, Rev. E	Development																				
	Submission																▲				
Deliverable: SAS System Requirement Specification, Rev. B	Development																				
	Submission													▲							
Deliverable: PSAS System Requirement Specification, Rev. B	Development																				
	Submission													▲							
Regulator assessment																					
Target RO closure Date																					▲